



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,907	09/26/2003	Jeyhan Karaoguz	14829US02	9187
23446	7590	08/04/2005	EXAMINER	
MCANDREWS HELD & MALLOY, LTD			REVAK, CHRISTOPHER A	
500 WEST MADISON STREET			ART UNIT	PAPER NUMBER
SUITE 3400			2131	
CHICAGO, IL 60661			DATE MAILED: 08/04/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>
	10/672,907	KARAOGUZ ET AL.
	<b>Examiner</b>	<b>Art Unit</b>
	Christopher A. Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 24 March 2005.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-21 is/are rejected.
- 7) Claim(s) 8 is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_
- 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_
- 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_

## DETAILED ACTION

### ***Priority***

1. Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged.

### ***Claim Objections***

2. Claim 8 is objected to because of the following informalities: It is recited that the processor comprises at least one of a personal computer and a set top box. It appears that the language should recite that the personal computer or set top box comprise a processor, not the processor comprising a personal computer or a set top box.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-5 and 7-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Inoue et al, U.S. Patent 6,891,819 in view of Watkins et al, US 2002/0120871.

As per claim 1, it is disclosed by Inoue et al of a method for theft prevention of communication devices used in a communication network (col. 1, lines 7-19 and col. 12, lines 21-28). The communication device deployed at a location that is communicatively coupled to the communication network is registered (col. 2, lines 55-60). Validation

Art Unit: 2131

information is entered relating to the communication device (col. 3, lines 16-31). The teachings of Inoue et al disclose of checking both validation information and registration information (col. 3, lines 16-31), but the teachings do not disclose of determining whether the communication device is authorized for use in the communication network. The teachings of Watkins et al disclose of determining whether or not the communication device is authorized for use in a communication network (page 1, paragraph 6). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to determine if a device is authorized for communicating within a protected communication network. The teachings of Watkins et al recite motivation for determining if devices are authorized for communications by disclosing that a problem exists in the prior art whereby client-server communications are susceptible to attacks (page 1, paragraph 4) and this is overcome by examining the properties of the client computer rather than behavior of a potential imposter (page 1, paragraph 5 and page 10, paragraph 106). It is obvious that the teachings of Inoue et al would have been further protected against theft by ensuring that a communication device is authorized for communicating in a communications network as is disclosed by Watkins et al.

As per claim 2, it is taught by Inoue et al of registering the communication device includes entering a password (col. 9, lines 2-14).

As per claim 3, Inoue et al discloses of entering a password as validation information (col. 10, lines 22-25).

As per claim 4, the teachings of Watkins et al disclose of locking the communication device out of the communication network upon a determination that the device is unauthorized (page 9, paragraph 91 and as shown in Figure 8). The teachings of Watkins et al are relied upon for determining whether or not the communication device is authorized for use in a communication network, please refer above for motivational benefits of applying this feature to the teachings of Inoue et al.

As per claim 5, it is taught by Inoue et al of determining the location of the communication device (col. 3, lines 17-24).

As per claim 7, Inoue et al discloses of a system supporting theft prevention of communication devices used in a communication network (col. 1, lines 7-19 and col. 12, lines 21-28). A home agent is connected to the communication network and receives information related to a communication device (col. 2, lines 55-60). It is inherent that the home agent comprises a processor since it is the computational and control unit of a computer that is responsible for reading and interpreting instructions for execution. Validation information is entered relating to the communication device and is then analyzed (col. 3, lines 16-31). The teachings of Inoue et al disclose of checking both validation information and registration information (col. 3, lines 16-31), but the teachings do not disclose of determining whether the communication device is authorized for use in the communication network. The teachings of Watkins et al disclose of determining whether or not the communication device is authorized for use in a communication network (page 1, paragraph 6). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to determine if a device is

Art Unit: 2131

authorized for communicating within a protected communication network. The teachings of Watkins et al recite motivation for determining if devices are authorized for communications by disclosing that a problem exists in the prior art whereby client-server communications are susceptible to attacks (page 1, paragraph 4) and this is overcome by examining the properties of the client computer rather than behavior of a potential imposter (page 1, paragraph 5 and page 10, paragraph 106). It is obvious that the teachings of Inoue et al would have been further protected against theft by ensuring that a communication device is authorized for communicating in a communications network as is disclosed by Watkins et al.

As per claim 8, it is disclosed by Inoue et al that the home agent (comprising a processor) is a personal computer (col. 7, lines 18-31).

As per claim 9, the teachings of Inoue et al disclose of a system supporting theft prevention of communication devices used in a communication network (col. 1, lines 7-19 and col. 12, lines 21-28). A communication device is deployed in a home environment (col. 4, line 60 through col. 5, line 5). The communication network communicatively coupled to the home environment to receiving authorization information (col. 4, line 60 through col. 5, line 18). The teachings of Inoue et al are silent in disclosing the step of determining whether the communication device is authorized for use in the communication network and to grant access is authorized. The teachings of Watkins et al disclose of determining whether or not the communication device is authorized for use in a communication network, and if authorized, access is permitted (page 1, paragraph 6 and as shown in Figure 8). It

would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to determine if a device is authorized for communicating within a protected communication network. The teachings of Watkins et al recite motivation for determining if devices are authorized for communications by disclosing that a problem exists in the prior art whereby client-server communications are susceptible to attacks (page 1, paragraph 4) and this is overcome by examining the properties of the client computer rather than behavior of a potential imposter (page 1, paragraph 5 and page 10, paragraph 106). It is obvious that the teachings of Inoue et al would have been further protected against theft by ensuring that a communication device is authorized for communicating in a communications network as is disclosed by Watkins et al.

As per claims 10 and 17, it is disclosed by Inoue et al that the communication network comprises a home network (closed communication infrastructure)(col. 3, lines 12-16).

As per claims 11 and 18, the teachings of Inoue et al recite that the communication network comprises the Internet (col. 7, lines 10-14).

As per claims 12 and 19, Inoue et al discloses of the communication network comprising a home network (closed communication infrastructure)(col. 3, lines 12-16).

As per claims 13 and 20, Inoue et al teaches that the authorization information comprises a password (col. 10, lines 22-25).

As per claims 14 and 21, it is disclosed by Inoue et al that the communication device comprises a personal computer (col. 2, lines 55-60).

As per claim 15, the teachings of Inoue et al disclose of a system supporting theft prevention of communication devices used in a communication network (col. 1, lines 7-19 and col. 12, lines 21-28). A storage device resides in a first home environment (col. 1, line 66 through col. 2, line 3 and as shown in Figure 1). A media device resides in a second home environment (col. 1, line 66 through col. 2, line 3 and as shown in Figure 1). A communication network communicatively coupled to the first home environment and the second home environment (col. 4, line 60 through col. 5, line 5). The communication network communicatively coupled to the home environment to receiving authorization information (col. 4, line 60 through col. 5, line 18). The teachings of Inoue et al are silent in disclosing the step of determining whether the communication device is authorized for use in the communication network and to grant access is authorized. The teachings of Watkins et al disclose of determining whether or not the communication device is authorized for use in a communication network, and if authorized, access is permitted (page 1, paragraph 6 and as shown in Figure 8). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to determine if a device is authorized for communicating within a protected communication network. The teachings of Watkins et al recite motivation for determining if devices are authorized for communications by disclosing that a problem exists in the prior art whereby client-server communications are susceptible to attacks (page 1, paragraph 4) and this is overcome by examining the properties of the client computer rather than behavior of a potential imposter (page 1, paragraph 5 and page 10, paragraph 106). It is obvious that the teachings of Inoue et al

would have been further protected against theft by ensuring that a communication device is authorized for communicating in a communications network as is disclosed by Watkins et al.

As per claim 16, the teachings of Inoue et al disclose of the communication network communicatively coupled to the home environment to receiving authorization information (col. 4, line 60 through col. 5, line 18). Watkins et al discloses of determining if the communication device is authorized for use in a communication network, and if authorized, access is permitted (page 1, paragraph 6 and as shown in Figure 8). The teachings of Watkins et al are relied upon for determining whether or not the communication device is authorized for use in a communication network, please refer above for motivational benefits of applying this feature to the teachings of Inoue et al.

5. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Inoue et al, U.S. Patent 6,891,819 in view of Watkins et al, US 2002/0120871 in further view of Ishikoff, U.S. Patent 5,748,084.

Inoue et al discloses of determining the location of the communication device (col. 3, lines 17-24). The combined teachings of Inoue et al and Watkins et al fail to disclose of notifying an authority of the location of the communication if it has been reported stolen. Ishikoff discloses notifying an authority of the location of a stolen device that has been reported stolen (col. 1, lines 59-65 and col. 3, lines 47-54). It would have been obvious to a person of ordinary skill in the art at the time of the

Art Unit: 2131

invention to have been motivated to provide authorities with information that can aid in the retrieval of stolen devices. The teachings of Ishikoff recite motivation for aiding in the retrieval of stolen devices by disclosing it can expedite in the return of the stolen device and furthermore, can assist in the capture of the thief to act as a deterrent against theft (col. 2, lines 60-66). It would have been obvious that the combination of the teachings of Inoue et al and Watkins et al would have been further secured against theft by applying the teachings of Ishikoff as a measure to aid in the retrieval of stolen devices.

### ***Conclusion***

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cain et al, U.S. Patent 6,507,914 discloses of reporting device information in order to facilitate in the recovery of a stolen device.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR  
  
July 29, 2005

Christopher Revak  
AU 2131  
  
7/29/05